Review on: WIFI Security and Attacks

Kartik Sahu
CIISE. Concordia University
Montreal, Canada
kartik.sahu@mail.concordia.ca

Syeda Maria Anjum
CIISE. Concordia University
Montreal, Canada
syedamaria.anjum@mail.concordia.ca

Pooja Polampalli
CIISE. Concordia University
Montreal, Canada
poojapolampalli14@gmail.com

Viraj Bhanushali
CIISE. Concordia University
Montreal, Canada
veerajgori@gmail.com

***Abstract*— The Users want connectivity regardless of their geographic position so that they can complete their tasks, and this has contributed to the rise in popularity of wireless networks. Wireless networks offer several advantages over wired networks, including greater mobility, greater flexibility, and lower costs.**

Wireless networks have a few benefits, but they also have a few security flaws. These flaws can generally be broken down into three categories: confidentiality, integrity, and availability. Wireless networks are susceptible to security flaws. A survey on attacks against wireless networks is presented, in which various security methods that help in protecting against different types of attacks are discussed, as well as the research areas that need to be concentrated for further development. Wired networks do not provide the same level of flexibility and scalability as wireless ones. Wireless networking has been able to overcome the difficulties that the wired network presented, and it also offers an easier deployment option.

***Index Terms*—** *Wireless security, wireless networks, PTW Attack, KoreK Attack and Sybil attacks.*

I. Introduction

In recent years, wireless networks have developed into an integral part of the day-to-day lives of a significant number of people. In particular, technical terms such as "Wi-Fi Fidelity"[1] have been utilized as nouns for a considerable amount of time. Despite the fact that the implementation of the physical and link layers of Wi-Fi is quite complicated, it is not uncommon for networks to be attacked using Wi-Fi. These attacks are based on the protocol. This is because there is such widespread adoption of Wi-Fi. It is possible to say that the risk that is posed by wireless networks is always present in our modern society. As a consequence of this, it is absolutely necessary to conduct research and analysis on the attacks that are associated with Wi-Fi networks. The purpose of this paper is to find and analyze the preventative measures that can be taken against threats to the security of wireless networks. This will be accomplished by researching and analyzing the cyberattack behaviours that are related to Wi-Fi in order to make wireless networks more secure. In particular, the focus of the paper will be on locating and examining the preventative measures that can be taken against threats to the safety of wireless networks. For the purpose of conducting research for this paper, case studies and reports are going to be the primary sources of information. Conducting research on actual instances of attacks on wireless networks was the first step in developing an accurate understanding of the enormous impact of this threat. This was the first step in developing an accurate understanding of the enormous impact of this threat. In order to address both the technical challenges and the legal concerns in an understandable manner, it is necessary to first conduct an analysis of the methods of attack used by the attacker, as well as any protocol security flaws, design defects, etc. This will protect wireless networks from potential threats to their security. In conclusion, some effective preventative measures in response to these threats are proposed here.

When we talk about wireless security, we are referring to the prevention of unauthorized access to wireless networks, devices, and data as well as the repair of any breaches that may occur. It entails utilizing a variety of strategies and practices that are designed to protect the availability, integrity, and confidentiality of wireless networks as well as the resources that are contained within them[1].

Because of the numerous potential dangers that can befall wireless networks, such as eavesdropping, data theft, denial of service (DoS) attacks, and malware infections, ensuring the security of wireless networks is of the utmost importance. If adequate security measures are not in place, it is very simple for unauthorized users to connect to a wireless network and use its resources. Once they have gained access, they are able to steal sensitive data and cause disruptions to the network's operations.

In order to protect data while it is in transit and to stop unauthorized access to wireless connections, stringent authentication procedures, encryption protocols, access control rules, intrusion detection and prevention systems, and other security measures are required to be put into place.

II. Background Overview-WEP,WPA,WPA2

The hardware, software, and protocols that guard wireless networks against unauthorized access, theft, and various other forms of cybercrime are collectively referred to as "wireless

security." Radio waves are used to transmit the data that is sent over a wireless network, and these waves can be picked up by any device that is within range. Eavesdropping, unauthorized access, and theft are all common problems associated with wireless networks because of this. Utilizing security measures such as encryption protocols, access control rules, and authentication procedures is required in order to protect these wireless networks from being compromised by unauthorized users.

Cellular networks, wireless local area networks (LANs), and sensor and communications networks are all examples of wireless networks; however, Wi-Fi is the wireless network protocol that is used the most frequently today.

Wired Equivalent Privacy, also known as WEP, Wi-Fi Protected Access, also known as WPA, and Wi-Fi Protected Access 2 are all examples of common wireless security protocols (WPA2). The earliest protocol, known as WEP, is no longer recommended because of the ease with which it can be broken. On the other hand, updated versions of WEP called WPA and WPA2 were made available to the general public.

WPA2 has overtaken its predecessor as the most widely used protocol because of the superior security afforded by its use of the AES encryption method. WPA3 is the most recent protocol, but despite having superior security features such as stronger encryption, protection from dictionary attacks, and simpler configuration of IoT devices, it hasn't caught on with users just yet. This is despite the fact that WPA3 is the newest protocol.

A robust security protocol is essential for securing wireless networks and maintaining the safety of private information. This is true regardless of the method that is utilized.

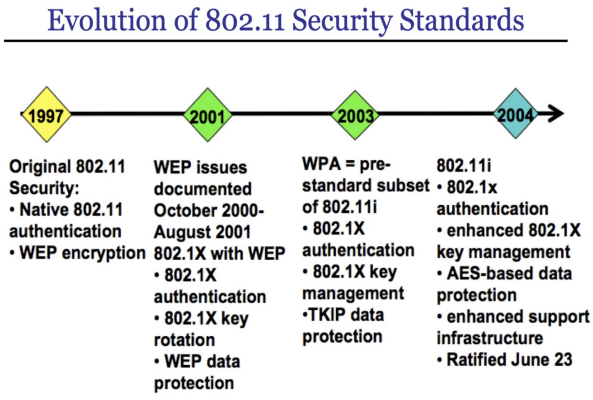


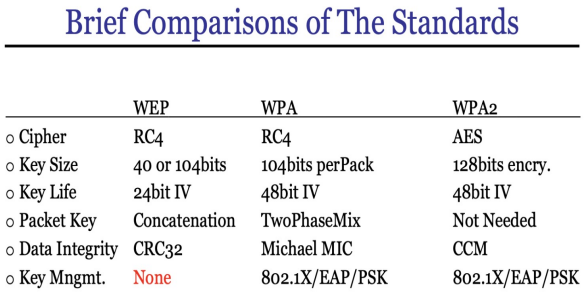
Fig. 1. Evolution of 802.11 Security Standards

How exactly does encryption for wireless communication work?

For the most part, the security of the data stored on wireless networks is ensured by cryptography, authentication, access control, and the detection and prevention of intrusions. These safeguards are in place to ensure that data is not snatched by unauthorized parties and to keep the network online and accessible at all times. In addition, these safeguards ensure that data is not compromised in any way.

The process of encoding information in such a way that it can be read only by those who are authorized to do so and who are in possession of the decryption key is known as encryption. Wireless networks have the ability to be encrypted using a variety of protocols, including WPA2 and WPA3.

Authentication procedures are used to verify the identities of users and the devices they use before allowing them to connect to a network. This is necessary before a connection can be made. Users are required to enter a password or passphrase before they are able to connect to a wireless network that employs a security protocol such as Wi-Fi protected access (WPA), for example.



	WEP	WPA	WPA2
○ Cipher	RC4	RC4	AES
○ Key Size	40 or 104bits	104bits perPack	128bits encry.
○ Key Life	24bit IV	48bit IV	48bit IV
○ Packet Key	Concatenation	TwoPhaseMix	Not Needed
○ Data Integrity	CRC32	Michael MIC	CCM
○ Key Mngmt.	None	802.1X/EAP/PSK	802.1X/EAP/PSK

Fig. 2. Comparison between WEP, WPA and WPA2

The access control rules detail not only the people who are authorized to connect to the network but also the privileges that are granted to those people once they have successfully established a connection. When it comes to putting in place access controls, there are a number of different factors that can be taken into consideration. These include the level of security, the type of device, and the user roles. Allowlisting and denylisting are two examples of access controls that are commonly found in wireless routers. The vast majority of network access control (NAC) solutions can be used with wired as well as wireless networks.

When it comes to the safety of wireless networks as a whole, the level of protection afforded to individual devices is also an essential component. Implement ing security policies, such as requiring all devices that connect to the network to have antivirus software, operating systems that are kept up to date, and VPN connections, is a good way to ensure the safety of the network as well as the users who use it. This protects both the network and the individuals who make use of it. One of the steps that must be taken in order to improve the safety of one's own mobile device is to restrict access to the administrator account. This is one of the steps that must be taken. There are also some other steps.

Monitoring a network in order to identify any possible intrusions is the job of intrusion prevention and detection systems (IPS). These systems are equipped with the intelligence necessary to identify malicious software, attempts at intrusion, and other forms of wireless attacks.

Investigate a Few of the Most Effective IDS/IPS Systems That Are Currently Available on the Market

The inner workings of each of the many different wireless security protocols.

The data that is sent over wireless networks is encrypted using wireless security protocols so that hackers and other eavesdroppers cannot access it and listen in on private conversations. In addition to this, they provide authentication

mechanisms, which are employed to ascertain the authenticity of clients and endpoints that are attempting to gain access to a network. Authentication mechanisms are offered by these companies. These protocols are responsible for enforcing access control rules in order to determine which users and devices can connect to the network and at what level of connectivity they are allowed.

The Wired Equivalent Privacy protocol employs the RC4 encryption algorithm in conjunction with a shared-key authentication mechanism in order to maintain confidentiality of transmitted data (WEP). 1997 marked the beginning of the use of this protocol, but it is no longer utilized as it is thought to be unsafe and is out of date. The year 1997 marked the beginning of the use of this protocol.

The Wi-Fi Protected Access standard, also known as WPA, was initially presented in 2003 with the intention of succeeding the WEP protocol. There are many different security features available, such as ensuring that messages have not been tampered with and enhancing the way that keys are managed. However, despite the fact that the Temporal Key Integrity Protocol (TKIP) is used to encrypt data in WPA, the protocol does not offer complete protection against hacking.

Wi-Fi Protected Access II (also known as WPA2), which was initially presented to the public in 2004, is still the wireless security protocol that the majority of people choose to make use of. It makes use of the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is itself based on the Advanced Encryption Standard (AES) encryption algorithm, in order to further enhance the already high level of security that the system possesses. WPA2 is essentially an improved version of the original WPA protocol, featuring improved management and decreased vulnerability to attack. WPA was originally designed to protect wireless networks from being intercepted by hackers.

Wi-Fi Protected Access III is the name of the most recent wireless security protocol that has been developed (WPA3). It provides additional layers of protection by way of enhanced encryption, defence against dictionary attacks, and data encryption that can be tailored to the user's specific requirements. Wi-Fi Easy Connect is a feature of WPA3 that was released in 2018, and it was designed to simplify the process of configuring devices, such as Internet of Things gadgets, that have a display interface that is either minimal or nonexistent. In order for the Internet of Things device to achieve this objective, it may provide the user with either a Quick Response (QR) code or a Near Field Communication (NFC) tag. After that, the user can make use of their own device to scan the shown code in order to establish a safe connection to the Wi-Fi network. Despite the fact that enhancements have been made, such as more robust encryption and safer key exchange, WPA3 has not yet found widespread adoption despite these enhancements.

When talking about the prevention of intrusions, breaches, and unauthorized access to wireless networks and services, the importance of wireless security cannot be overstated. Hackers can easily gain access to a wireless network that does not have adequate security, and while they are there, they can cause disruptions and steal confidential information.

It is essential to have strong authentication methods, encryption protocols, and access control policies in place in order to keep wireless networks secure. One of the most important aspects of wireless network security controls is making sure that the routers being used are secure and have been configured correctly. Intruder detection and prevention systems, as well as firewalls, are two examples of additional tools that can further increase network security.

Networks that employ WPA2 or WPA3 are ahead of the game in terms of security because significant advancements have been made in wireless security protocols over the course of the years. These advancements have occurred over the course of the years. It is possible to protect your wireless network from potential hackers and other unauthorized users by utilizing modern protocols, tools, and best practices in network security.

III. Types of Existing Attacks

It is essential to keep in mind that the aforementioned are merely a few examples of the various kinds of assaults that can be carried out against WEP, WPA, and WPA2. Because Wi-Fi security is an ever-evolving field, and because new attacks are continually being developed, it is essential to stay informed about the most recent threats and vulnerabilities.

The following are the most common types of attacks on WEP, WPA, and WPA2:

WEP:

1. *Passive Attack:* The first step in a passive attack is to monitor the traffic on the wireless network in search of packets that contain the encryption key.

An example of a passive attack on WEP would be to monitor wireless traffic in search of packets that contain the encryption key (Wired Equivalent Privacy). An adversary would require possession of the encryption key that was used to encrypt the data prior to its transmission over the wireless network in order to be able to decrypt any and all encrypted network traffic.

An essential component of a passive attack on WEP is the gathering of a sufficient number of data packets to make it possible for the attacker to speculate on the encryption key. By eavesdropping on wireless traffic and stealing data packets, the attacker can cause disruption to the network without actively affecting it. This can be accomplished without the attacker having to do anything to the network itself. Because of the ineffectiveness of the encryption algorithm that WEP employs, it is susceptible to passive attacks.

The following is an example of a passive attack against WEP:

The attack starts with the use of a wireless network adapter to snoop on wireless traffic in the area around the target network. The goal is to collect enough data packets to give the attacker enough information to make an educated guess as to what the encryption key is. After that, the attacker employs a piece of software such as Aircrack-ng to perform an analysis on the captured packets in order to discover the encryption key.

It is important to keep in mind that passive attacks on WEP are easy to put into action, and that even an inexperienced attacker can capture and examine wireless traffic with the assistance of a number of different tools that are easily accessible.

Because of this, WEP is a very insecure protocol, and modern wireless networks should avoid using it at all costs.

The goal of an attacker conducting a passive attack is to obtain the information that is being sent or received over a network. Because the attacker does not make any changes to the

information, passive attacks are notoriously difficult to detect [5].

The following is an explanation of some of the passive attacks:

- Traffic Analysis: Traffic analysis is the process of probing messages to infer information from various patterns of message transmission. [15] Traffic analysis is also known as message traffic analysis. Computer security experts are concerned about the practice of traffic analysis, which can be performed within the context of military or pattern-of-life analysis. To protect against these kinds of assaults, countermeasures are taken at the transport level. These countermeasures include encrypting messages, employing a limited form of message rerouting, delaying messages, and sending dummy messages as required within resource capacities.
- Eavesdropping: Eavesdropping focuses on capturing small packets from the network that are being transmitted by other computers and reading the data content in search of any type of information. Eavesdropping can be done in a number of ways. Because this attack does not utilize any form of encryption, it is significantly more effective. Because it is difficult to know when they are occurring, eavesdropping attacks are dangerous. Installing monitoring software on the client system can protect it from the eavesdropping attack. This software helps the attacker collect all of the information they require to carry out the attack successfully. Eavesdropping can occur at any point along this network thanks to these devices. One additional method involves the utilization of encryption between the client and the server.

2. *Active Attack:* This type of attack involves actively sending a data packet that is designed to contain the encryption key through the wireless network in order to gain access to it.

An adversary needs to "seed" a WEP-protected wireless network with fake data before they can gain access to the encryption key for the network and launch an active attack against it. An adversary who is able to generate new packets with the encryption key of a wireless network is able to read all encrypted traffic that is taking place on the network. This is due to the fact that the encryption key of a wireless network is used to encrypt and decrypt data while it is in transit.

An active attack against WEP has as its primary objective the flooding of the network with traffic in an effort to determine the encryption key. This is accomplished by using a variety of different methods. Active attacks are able to be launched against WEP as a result of the relatively low level of security provided by its encryption algorithm.

The following is an illustration of an active assault on WEP:

The attacker starts by flooding the target network with forged data packets that are designed to exploit flaws in the WEP encryption algorithm. These flaws can be exploited to gain access to the network. This action is taken in preparation for gaining access to the network. When a response is sent by the network, the encryption keys are included in that response. These encryption keys can be intercepted and analyzed with a tool like Aircrack-ng in order to discover the key. This can be done in order to discover the key.

If a potential threat obtains knowledge of the encryption key, they will be able to decipher any data that was encrypted on the network using that key once they have access to that key.

Because the attacker has access to this information, they are in a position to intercept data while it is in motion, which gives them the ability to steal passwords and other sensitive information.

Attacks against WEP that require the attacker to actively interact with the network in order for the attack to be successful are significantly more difficult than passive attacks. Even though there are many tools that make it simple for even an inexperienced attacker to generate and analyze traffic on a wireless network, these attacks continue to be incredibly simple to carry out despite the availability of such tools. Despite the fact that there are many tools that make it simple for even an inexperienced attacker to generate and analyze traffic on a wireless network. Because of this, the WEP protocol is a very insecure one, and modern wireless networks should do everything in their power to stay away from using it.

3. *WEP Key Cracking* is the process of attempting to acquire a key to an encryption system by employing either a dictionary attack or brute force.

An adversary could try to break into a wireless network protected by WEP (Wired Equivalent Privacy) by employing a brute force attack or a dictionary attack in an effort to decipher the network's encryption and gain access to the network. However, if an adversary successfully breaks the encryption key, they will be able to read the data even though it is transmitted over a wireless network in an encrypted format.

In order to determine the encryption key for WEP, the method of trial and error is utilized as part of the cracking process. Because the length of the encryption key is always the same, the WEP encryption algorithm is susceptible to brute-force attacks. This is because the key length is always the same (64 bits or 128 bits).

A WEP key can be decrypted using the steps listed below:

An attacker needs to obtain a sufficient number of data packets from the network first, then analyze the data packets using a tool such as Air cracking, and finally, the attacker needs to guess the encryption key in order to break into a wireless network.

Both "brute force," which means trying each and every possible combination of the key, and "dictionary," which means using a list of possible keys that has been precomputed, are common methods for breaking encryption. "Brute force" refers to trying each and every possible combination of the key, while "dictionary" refers to using a list of possible keys.

If a potential danger is able to get their hands on the encryption key, they will be able to decrypt any data, including passwords, that was encrypted before being sent over the network. This includes the data that was sent over the network.

Because there are so many tools available, it is simple for even an inexperienced attacker to capture and examine the traffic of wireless networks. In addition, attacks that are aimed at breaking WEP keys are not particularly difficult to carry out. WEP should not be used in modern wireless networks as it has all of these security flaws that make it insecure.

WPA/WPA2:

1. *Brute Force Attack:* In this type of attack, the hacker tries to guess the password by cycling through a large number of different possible combinations.

Using a powerful computer or network of computers, a brute force attack on WPA/WPA2 involves trying every possible combination of characters until the correct passphrase that is used to secure the wireless network is found. If an attacker were to crack the passphrase, they would be able to decrypt all of the network traffic that has been encrypted using that passphrase. This is because the passphrase is used to encrypt and decrypt data that is transmitted over the wireless network.

An attack using brute force on WPA or WPA2 involves attempting to guess the passphrase by cycling through a large number of possible combinations in an effort to do so. Because WPA and WPA2 use a robust encryption algorithm and a passphrase with a variable length (up to 63 characters), brute force attacks can be very time-consuming and may require a significant amount of computing power to carry out successfully.

An attack using brute force on WPA or WPA2 would look something like this:

• The adversary retrieves a handshake packet from the wireless network and examines it. A wireless access point and a device that is trying to connect to a network exchange something called a "handshake packet." This is a special packet that is exchanged between the two parties. The handshake packet has encrypted information in it that can be used to try and figure out the passphrase.

• The attacker examines the handshake packet that was captured with a tool like Aircrack-ng and then makes an attempt to guess the passphrase using the information gained from this examination.

An attacker may resort to a brute force attack, which involves attempting each and every possible combination of characters until the correct passphrase is discovered.

• The attacker may also use a dictionary attack, which involves iteratively searching through a pre-computed list of possible passphrases until the correct one is discovered.

As soon as the correct passphrase has been identified by the adversary, they are able to use it to decrypt all of the network traffic that has been encrypted using that passphrase. •

After gathering this information, the attacker is in a position to steal sensitive data or information, such as passwords or other data that is being transmitted over the network.

It is essential to be aware that brute force attacks on WPA and WPA2 can require a significant amount of computing power and can take a significant amount of time to carry out. Nevertheless, brute force attacks are still a potential threat to wireless networks that are secured with weak passphrases. This is because powerful computers and the resources of the cloud can be used to perform brute force attacks. Because of this, it is essential to utilize passphrases that are both robust and complex and to periodically change them in order to reduce the risk of being subjected to brute force attacks.

2. *Dictionary Attack:* A dictionary attack is a type of attack that involves trying a large list of common passphrases or words until the correct passphrase is found. This type of attack is known as a brute force attack. An application like Aircrack-ng is utilized by the adversary in order to automate the process of attempting each passphrase listed in the dictionary until the correct one is discovered. It is possible for this kind of attack to be successful if the passphrase that is used to secure the wireless network is either not very strong or is easy to figure out.

3. *Sybil attacks:* A Sybil attack is an attack in which a node pretends to be more than one node by forging the identities of other nodes.

The integrity of the data, as well as the security and utilization of the resources, can all be jeopardized by this kind of attack. When entities are assumed to have exactly one identity, this kind of attack can occur in distributed peer-to-peer systems. The vulnerability of the system to sybil attacks is determined by whether or not this assumption is true. The most significant drawback is that it is more difficult to be detected in the network, which causes an excessive amount of communication overhead and raises the potential risk. In addition, this raises the likelihood that an attack will succeed.

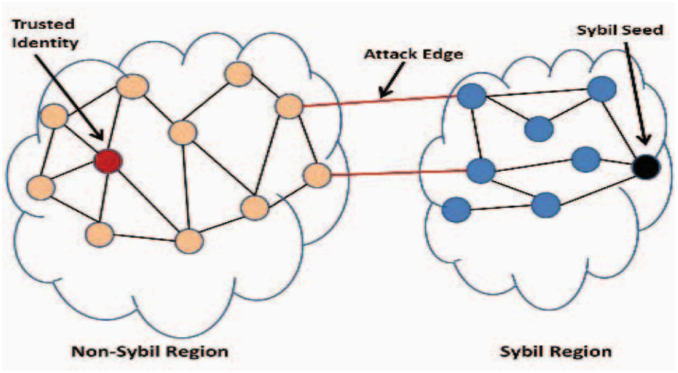


Fig. 3. Sybil Attack

Validation strategies have the potential to be beneficial in the fight against Sybil attacks. An entity and an identity can reach a secure one-to-one agreement through the use of a central authorization, which can even cause a seek for invalidation if a remote id is acknowledged by a local id that relies on the central authorization. These methods are wholly reliant on a person's identity in either an indirect or direct manner, depending on your preference.

When direct validation is performed, the local entity will inquire with the central authorization in order to validate the remote entity. Only approved identities, which in turn support remote identities for indirect validation, are necessary for the entity to function properly.

4. *Rogue Access Point Attack* Variation The rogue access point attack has a variant known as the evil twin attack. In this type of attack, the attacker creates a fake access point that has the same name (SSID) and security settings as the genuine access point in the hopes that users will connect to the fake access point instead of the legitimate one. Once they are connected, attackers have the ability to intercept and capture network traffic, which includes sensitive information such as usernames and passwords. This kind of attack may be successful if the attacker is able to create an access point that has the same name as the legitimate access point, the same security settings, and a stronger signal than the legitimate access point.

5. *WPS Attack:* WPS, which stands for "Wi-Fi Protected Setup," is a feature of some wireless routers that enables users to connect to the network quickly and easily without being required to enter a passphrase. However, this feature can also be exploited by hackers. On the other hand, it has been discovered that WPS has a number of flaws that can be taken advantage of in order to gain access to a network. The goal of a WPS attack is to guess the WPS PIN and gain access to the network. This is accomplished by exploiting the vulnerabilities described above. It is possible for this kind of attack to be successful if the router has WPS enabled and the PIN is either not strong enough or is easy to guess.

It is essential to keep in mind that these attacks have a chance of succeeding if the wireless network in question does not have adequate security measures in place or if the person attempting the attack is equipped with sufficient knowledge and resources to carry it out. It is essential to employ passphrases that are robust and convoluted, to ensure that the software and firmware of the wireless network are always up to date, and to perform routine checks to look for suspicious activity on the network. Only then will you be able to protect yourself from these attacks. Users should also exercise caution before connecting to unfamiliar wireless networks and should only connect to networks in which they have complete faith.

IV. PTW Attack-An Overview

Pyshkin-Tews-Weinmann is an attack that is frequently used when trying to break the WEP (Wired Equivalent Privacy) encryption. This attack, which is based on statistical analysis of the WEP key stream, can be used to successfully recover the WEP key with a high rate of success.

For the PTW attack to be successful, it is necessary to capture a significant amount of traffic that is encrypted using the target WEP key. When you have the traffic that has been captured, you can use specialized software such as Aircrack-ng or the Aircrack-ng plugin for Wireshark to decrypt the WEP key.

The PTW attack is an outdated method for breaking the WEP encryption, and it has a number of security holes that make it vulnerable to attack. To begin, it is ineffective unless a significant amount of targeted traffic is captured, which, depending on the specifics of the situation, may be difficult to accomplish. Second, the PTW attack is only capable of breaking the WEP encryption method, which is now considered to be unreliable and obsolete. The encryption protocols, such as WPA2 and WPA3, that are utilized by modern Wi-Fi networks make them significantly more resistant to brute-force attacks.

Keep in mind that attempting to decrypt a WEP-protected network without the permission of the owner is not only against the law but also unethical. In addition, it is against the law in many countries to use a Wi-Fi network that is not secure without first obtaining permission to do so. Connecting to only encrypted Wi-Fi networks is the best way to safeguard your private information and identity while you're online.

The Wireless Encryption Protocol, also known as WEP, is a standard used by businesses all over the world to secure wireless networks. Its widespread adoption at the dawn of the Wi-Fi era belies the fact that its security can be easily breached using the appropriate instruments and procedures. The Pyshkin-Tews-Weinmann attack, also known as the PTW attack, is one of the most effective techniques for breaking the WEP encryption.

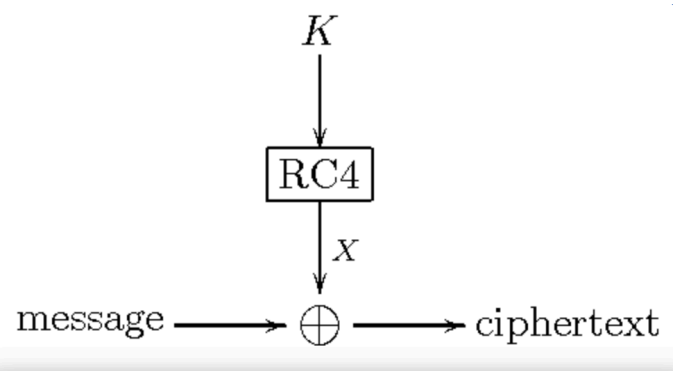


Fig. 4. RC4 Stream cipher

The statistical PTW attack aims to exploit any vulnerabilities that may exist within the WEP encryption algorithm. The WEP encryption algorithm, RC4, is deciphered by analyzing this keystream. To generate the ciphertext from the plaintext, XOR operations are performed using the bytes that make up the RC4 keystream. The PTW attack can be used to gain statistical insight into the keystream in situations where multiple packets are encrypted using the same keystream.

For the PTW attack to be successful, it is necessary to capture a significant amount of encrypted traffic using the target WEP key. Your chances of being successful will improve if you attract a larger number of visitors. Using programs such as Airodump-ng and Kismet, it is possible to record the traffic that is transmitted over a Wi-Fi network and save it to a file.

When the traffic has been captured, the next step is to retrieve the keystream from each individual packet. Instruments such as Airdecap-ng and the Aircrack-ng plugin for Wireshark are helpful for accomplishing this objective. The keystream of each packet is retrieved by the tool and written to a file.

You can use a tool like Aircrack-ng to examine the keystreams and try to decipher the WEP key once you have them in hand. Aircrack-ng analyzes the keystreams with a number of different statistical methods to determine the WEP key. The PTW attack is one of the many techniques that are utilized by Aircrack-ng.

The attacker can construct a statistical profile of the keystream, which can then be used to recover the key with a high degree of accuracy using the PTW attack. Despite this, there are a few drawbacks to it. To begin, a significant quantity of targeted traffic must be captured in order for it to be successful. The more people who visit your site, the better. Second, the PTW attack is ineffective against any encryption except for the WEP standard. The encryption protocols used by modern Wi-Fi networks, such as WPA2 and WPA3, are much more resistant to brute-force attacks than their predecessors.

It is important to keep in mind that attempting to crack WEP encryption without the permission of the network owner is both

unethical and illegal. It is against the law in many countries to use a public Wi-Fi network without first obtaining permission from the network's owner. Connecting to only encrypted Wi-Fi networks is the best way to safeguard your private information and identity while you're online.
Together, the wireless access point (AP) and the wireless client devices create an encrypted network by employing a secret key that is only known to themselves. The RC4 algorithm and the key are used to encrypt the data before it is transmitted over the wireless network.

The vulnerability of the WEP encryption method to statistical attacks and the fact that it only uses a single encryption key for all network traffic are both examples of its shortcomings. This vulnerability is exploited by the PTW attack, which does so by inspecting the keystream that the RC4 algorithm produces.

The plaintext is XORed with the keystream, which is a sequence of pseudo-random bytes generated by the RC4 algorithm. This process is repeated so that the ciphertext can be created. Because the same keystream is used to encrypt each and every packet that is sent across the network, an adversary who is successful in stealing a sufficient number of packets can use statistical methods to figure out the secret WEP key by analyzing the keystream.

In order to successfully carry out a PTW attack, the adversary needs to first seize a sizeable quantity of encrypted packets that are being sent across the network using the intended recipient's WEP key. After that, the attacker will extract the keystream from each packet and examine it for patterns and collisions.

The situation that occurs when two keystreams share an element that can be used to figure out the WEP key is referred to as a "collision," and the term "collision" refers to the situation. An adversary can piece together information about the WEP key by analyzing many pairs of keystreams and looking for collisions. This allows the adversary to piece together information about the WEP key.

In conclusion, the PTW attack is a statistical attack that decrypts wirelessly transmitted data by taking advantage of flaws in the WEP encryption algorithm. These flaws can be found in the WEP encryption algorithm. Although the PTW attack is a potent means of breaking WEP security, it is ineffective in the face of newer encryption standards like WPA2 and WPA3. It is not only unethical but also against the law to try to decrypt a network by using a WEP key unless you have the permission of the network's owner.
The statistical PTW (Pyshkin-Tews-Weinmann) attack is capable of breaching the security provided by the WEP encryption algorithm. It is possible to carry out this attack due to the fact that the WEP encryption algorithm reuses the same keystream for each and every packet that is transmitted over a wireless network.

The RC4 algorithm generates a stream of pseudo-random bytes called the keystream, which is then used to encrypt the data in each packet. Since the same keystream is used for each packet, an attacker who manages to steal enough of them can use statistical methods to deduce the secret WEP key.

Because it compares two keystreams in the search for a particular pattern known as a "collision," the PTW attack is effective. If two keystreams are found to be in collision with one another, this indicates that they share some information in common that can be used to deduce the WEP key. An adversary can obtain the WEP key by analyzing a sufficient number of keystream pairs and searching for collisions. This allows for the key to be recovered.

Capturing a large number of encrypted packets transmitted with the target WEP key is necessary for the PTW attack. A packet capture program like Wireshark or Airodump-ng can help with this. When the adversary has collected a sufficient number of packets, they can extract the keystream from each packet with the assistance of a program such as Airdecap-ng or Wireshark augmented with the Aircrack-ng plugin.

After the keystreams have been extracted, the WEP key can be determined by an attacker by using statistical methods to analyze the keystreams. The PTW attack incorporates both keystream analyses and collision detection into its methodology. By analyzing collisions between keystreams, which take place when two keystreams share some information in common with one another, we can acquire additional knowledge regarding the WEP key.

The PTW assault is dependent on the steps that are listed below:
• You will be able to amass a sizeable amount of keystream data if you collect a significant number of packets.
• The keystream must be extracted from each individual packet in order to fulfill the requirements.
• Compare the two keystreams in order to search for potential collisions.
• It is possible to discover the hidden WEP key by analyzing the data produced by the collisions.
Although the PTW attack is a powerful method for decrypting WEP, it does have a few limitations. It is not always easy to acquire a large volume of captured traffic, which is required for it to be effective. However, this is necessary for it to be effective. In addition, the PTW attack is currently only able to break the antiquated WEP encryption standard.
This is as a result of the fact that the encryption protocols utilized by contemporary Wi-Fi networks, such as WPA2 and WPA3, are noticeably more challenging to crack utilizing brute-force methods.
The Pyshkin, Tews, and Weinmann (PTW) attack, also known as the Aircrack-ng attack, is another cryptographic attack on Wired Equivalent Privacy (WEP) encryption. The PTW attack is an improvement over the earlier FMS attack and is even more efficient, requiring fewer packets to be captured to recover the WEP key. The PTW attack mainly exploits statistical weaknesses in the RC4 stream cipher and key scheduling algorithm (KSA) used in WEP.
To understand the PTW attack, let's first recap the basics of the WEP encryption mechanism:

- RC4 Stream Cipher: WEP uses the RC4 stream cipher for encryption. A key stream is generated by

combining a shared secret key (SK) with an Initialization Vector (IV). The key stream is then XORed with the plaintext to produce the ciphertext.

- Initialization Vector (IV): IV is a 24-bit value that changes for each packet sent over the network. It is combined with the shared secret key to produce the key used for RC4 encryption. The IV is transmitted in plaintext along with the encrypted data.
- Integrity Check Value (ICV): WEP includes an Integrity Check Value (ICV) in its encrypted payload. The ICV is a 32-bit checksum (based on CRC-32) calculated from the plaintext data, used to verify the integrity of the decrypted data.

Now let's dive into the details of the PTW attack:

1. Capture packets: An attacker passively captures a large number of encrypted packets transmitted over the wireless network.
2. Exploit statistical properties: The PTW attack exploits the fact that the RC4 cipher has certain statistical properties, which can be leveraged to recover the WEP key. In particular, the attack exploits the fact that the first few bytes of the RC4 key stream (generated by combining the shared secret key and the IV) exhibit biases, which can be used to recover the secret key.
3. Construct key hypotheses: The attacker constructs hypotheses for the shared secret key bytes based on the observed biases in the key stream bytes. The attacker examines the first two bytes of the key stream (Z[0] and Z[1]) and uses the captured IVs and ciphertexts to build hypotheses for the corresponding bytes of the shared secret key (K[0] and K[1]).
4. Use dynamic programming: The PTW attack employs dynamic programming to efficiently combine the key hypotheses and evaluate the likelihood of different key combinations. The attacker maintains a table of key candidate scores, updating the scores as more packets are captured and analyzed. The dynamic programming approach allows the attacker to avoid exhaustive search and quickly identify the most likely key values.
5. Key recovery: Once the attacker has collected enough packets and built a sufficient number of key hypotheses, the most likely candidate for the shared secret key can be recovered by selecting the key combination with the highest score.
6. ICV validation: To confirm the correctness of the recovered key, the attacker can decrypt the captured packets and check if the calculated ICV matches the decrypted ICV. If the ICVs match, the attacker has successfully recovered the correct WEP key.

The PTW attack is considered very efficient, requiring significantly fewer packets to be captured compared to the FMS attack. In some cases, the PTW attack can recover the WEP key with as few as 20,000 to 40,000 captured packets. This efficiency makes the PTW attack even more devastating for the security of WEP-protected networks.

The discovery of the PTW attack and other vulnerabilities in WEP has led to the protocol being deprecated in favor of more secure encryption protocols, such as WPA2 and WPA3. These modern encryption protocols utilize stronger cryptographic primitives and improved key management

To provide a mathematical and statistical explanation of the PTW attack, we need to examine the RC4 key scheduling algorithm (KSA) and the statistical properties that the attack exploits.

Recall that the RC4 algorithm has two main parts:

1. Key Scheduling Algorithm (KSA)
2. Pseudo-Random Generation Algorithm (PRGA)

We have already provided the mathematical explanation of these algorithms in the response to the FMS attack. The PTW attack focuses on the statistical biases in the PRGA, specifically in the first few bytes of the key stream.

Statistical Properties:

The PTW attack exploits the following statistical properties in the RC4 key stream:

The probability that the first byte of the key stream (Z[0]) equals the first byte of the secret key (K[0]) plus the second byte of the secret key (K[1]) is greater than 1/256.

The probability that the second byte of the key stream (Z[1]) equals the second byte of the secret key (K[1]) is greater than 1/256.

PTW Attack (Mathematical and Statistical Explanation):

The PTW attack uses these statistical properties to recover the shared secret key from the IVs and ciphertexts. The attack consists of the following steps:

- Capture packets and calculate key stream bytes: The attacker captures a large number of encrypted packets and calculates the first two bytes of the key stream (Z[0] and Z[1]) for each packet using the statistical properties mentioned above.
- Create a table of key candidates: The attacker creates a table to store the candidates for the shared secret key. For each captured packet, the attacker computes a set of possible key candidates based on the known IV, the ciphertext, and the statistical properties. The candidates are pairs of values for K[0] and K[1], computed using the following equations:

K[0] = Z[0] - IV[1] K[1] = Z[1]

- Update key candidate scores: The attacker maintains a table of key candidate scores, updating the scores as more packets are captured and analyzed. For each key candidate, the attacker computes the number of times the candidate satisfies the statistical properties and increments the corresponding score in the table.
- Dynamic programming: The PTW attack employs dynamic programming to efficiently combine the key hypotheses and evaluate the likelihood of different key combinations. The attacker maintains a table of key candidate scores, updating the scores as more packets are captured and analyzed. The dynamic programming approach allows the attacker to avoid an exhaustive search and quickly identify the most likely key values.
- Key recovery: After gathering enough packets and building a sufficient number of key hypotheses, the most likely candidate for the shared secret key can be recovered by selecting the key combination with the highest score:

(K[0], K[1]) = argmax_{K[0], K[1]} Score(K[0], K[1])

- ICV validation: The attacker can confirm the correctness of the recovered key by decrypting the captured packets and verifying the Integrity Check Values (ICVs).

In summary, the PTW attack exploits the statistical biases in the first few bytes of the RC4 key stream to recover the WEP key. By capturing a large number of packets and analyzing the IVs and ciphertexts, the attacker can construct key hypotheses and use dynamic programming to efficiently combine the hypotheses and evaluate the likelihood of different key combinations. Once the attacker has collected enough packets and built a sufficient number of key hypotheses, the most likely candidate for the shared secret key can be recovered by selecting the key combination with the highest score. The recovered key can then be validated by decrypting captured packets and verifying the Integrity Check Values (ICVs).

The PTW attack is highly efficient and effective, requiring fewer packets compared to the FMS attack to recover the WEP key. In some cases, the PTW attack can recover the WEP key with as few as 20,000 to 40,000 captured packets. The ability to recover the WEP key in such a short time makes the PTW attack a significant threat to the security of WEP-protected networks.

The discovery of the PTW attack, along with the FMS attack and other vulnerabilities, has led to WEP being deprecated in favor of more secure encryption protocols, such as WPA2 and WPA3. These modern encryption protocols utilize stronger cryptographic primitives and improved key management techniques, offering better security for wireless networks.

In conclusion, the PTW attack demonstrates the importance of understanding the statistical properties of cryptographic algorithms and the potential vulnerabilities that can arise from these properties. By exploiting the statistical biases in the RC4 key stream, the PTW attack can efficiently recover the WEP key, highlighting the need for more secure encryption protocols to protect wireless networks.

V. FMS Attack-An Overview

The Fluhrer, Mantin, and Shamir (FMS) attack is a type of cryptographic attack that exploits vulnerabilities in the Wired Equivalent Privacy (WEP) encryption protocol. WEP, introduced in 1999, aimed to provide a level of security equivalent to wired networks for wireless networks. However, it was soon discovered that WEP had several security flaws, making it vulnerable to attacks like the FMS attack.

To understand the FMS attack, we must first understand the basics of the WEP encryption mechanism:

1. RC4 Stream Cipher: WEP utilizes the RC4 stream cipher for encryption. In RC4, a key stream is generated by combining a shared secret key (SK) with an Initialization Vector (IV). The key stream is then XORed (bitwise exclusive OR) with the plaintext to produce the ciphertext.
2. Initialization Vector (IV): IV is a 24-bit value that changes for each packet sent over the network. It is combined with the shared secret key to produce the key used for RC4 encryption. The IV is transmitted in plaintext along with the encrypted data.
3. Integrity Check Value (ICV): WEP also includes an Integrity Check Value (ICV) in its encrypted payload. The ICV is a 32-bit checksum (based on CRC-32) calculated from the plaintext data. This is used to verify the integrity of the decrypted data.

Now, let's dive into the details of the FMS attack:

The FMS attack exploits weaknesses in the RC4 key scheduling algorithm (KSA) and the weak IVs generated by WEP. Due to the design of the KSA, certain IVs can cause the first few bytes of the key stream to have a higher probability of revealing information about the secret key.

The FMS attack follows these steps:

1. Capture packets: An attacker passively captures a large number of encrypted packets transmitted over the wireless network.
2. Identify weak IVs: The attacker analyzes the captured packets to identify weak IVs that leak information about the secret key. The weak IVs are identified based on specific patterns that cause the KSA to produce weak key streams.
3. Statistical analysis: The attacker uses statistical analysis to extract information about the secret key from the weak IVs. This is done by calculating the conditional probabilities for each possible value of the secret key bytes, given the observed weak IVs and their corresponding ciphertexts. By accumulating enough weak IVs, the attacker can reliably determine the secret key bytes.
4. Key recovery: Once enough secret key bytes are recovered, the attacker can reconstruct the complete WEP key (including the shared secret key and the remaining IVs). This allows the attacker to decrypt all traffic on the wireless network.
5. Integrity Check Value (ICV) validation: To confirm the correctness of the recovered key, the attacker can decrypt the captured packets and check if the calculated ICV matches the decrypted ICV. If the ICVs match, the attacker has successfully recovered the correct WEP key.

The FMS attack is considered extremely effective, as it can be performed with a relatively low number of captured packets (on the order of tens of thousands), making WEP encryption highly insecure. As a result, WEP has been deprecated, and modern wireless networks use more secure encryption protocols, such as WPA2 and WPA3.

To provide a mathematical and statistical explanation of the FMS attack, we need to examine the RC4 key scheduling algorithm (KSA) and the statistical biases that the attack exploits.

RC4 Algorithm:

Key Scheduling Algorithm (KSA):

1. Let S be a permutation of all 256 possible bytes (0 to 255). The KSA initializes S using the key (concatenation of the shared secret key and the IV):

Input: Key (K) of length L bytes

Output: Initialized permutation S of 256 bytes

```
S = [0, 1, ..., 255]
j = 0

for i in range(0, 256):
    j = (j + S[i] + K[i % L]) % 256
    swap(S[i], S[j])
```

Pseudo-Random Generation Algorithm (PRGA):

2. The PRGA generates a key stream by permuting S and XORing the output with the plaintext to create the ciphertext.

Input: Initialized permutation S

Output: Key stream Z of required length

```
i = j = 0
while generating key stream:
    i = (i + 1) % 256
    j = (j + S[i]) % 256
    swap(S[i], S[j])
    t = (S[i] + S[j]) % 256
    Z = S[t]
```

FMS Attack (Mathematical and Statistical Explanation):
The FMS attack exploits biases in the KSA when certain weak IVs are used. The weak IVs have a higher probability of causing the second byte of the key stream (Z[1]) to reveal information about the first byte of the shared secret key (K[0]). The attack focuses on the following correlation:

$$Pr(S[1] = K[0] \mid IV[0] = 3) \approx 5/256$$

This correlation states that, given a weak IV with its first byte (IV[0]) equal to 3, the probability that S[1] equals the first byte of the shared secret key (K[0]) after the KSA is about 5/256, which is significantly higher than the probability of 1/256 for a random permutation.
The FMS attack involves the following steps:

- Capture packets and identify weak IVs: The attacker captures a large number of encrypted packets and identifies weak IVs that have a higher probability of revealing information about the shared secret key, such as those with the first byte equal to 3.
- Construct conditional probabilities: The attacker calculates conditional probabilities for each possible value of the secret key bytes (K[i]), given the observed weak IVs and their corresponding ciphertexts (C[j]):

$$Pr(K[i] = x \mid IV, C[j]) = Pr(Z[j] = C[j] \oplus x \mid IV)$$

- Exploit statistical biases: The attacker exploits the statistical biases caused by weak IVs to accumulate evidence for the secret key bytes. For each weak IV and ciphertext pair, the attacker updates a count for each possible value of K[i] based on the observed correlations, such as the one mentioned earlier:

$$Count(K[i] = x) \mathrel{+}= Pr(K[i] = x \mid IV, C[j])$$

Key recovery: After gathering enough weak IVs and ciphertexts, the attacker can estimate the shared secret key bytes by selecting the values with the highest counts:

$$K[i] = \text{argmax}_x \, Count(K[i] = x)$$

- ICV validation: The attacker can confirm the correctness of the recovered key by decrypting the captured packets and verifying the Integrity Check Values (ICVs).

In summary, the FMS attack exploits statistical biases in the RC4 key scheduling algorithm when weak IVs are used, allowing the attacker to recover the shared secret key by analyzing a large number of encrypted packets. By calculating conditional probabilities and exploiting the correlations between weak IVs, key stream bytes, and ciphertext bytes, the attacker can accumulate evidence for the values of the secret key bytes. Once enough weak IVs are collected, the attacker can estimate the secret key bytes by selecting the values with the highest counts. The recovered key can then be validated by decrypting captured packets and verifying the Integrity Check Values (ICVs).
The success of the FMS attack highlights the importance of using secure encryption protocols in wireless networks. Since the discovery of the FMS attack and other vulnerabilities in WEP, the protocol has been deprecated in favor of more secure alternatives, such as WPA2 and WPA3. These modern encryption protocols utilize stronger cryptographic primitives and improved key management techniques, offering better security for wireless networks.

VI. Implementation

Link to GitHub: https://github.com/pooja-polampalli/INSE6120-2023-Project-WifiSecurity

Prerequisite:

- A Linux-based operating system (such as Kali Linux) with Aircrack-ng installed.
- A wireless adapter is capable of packet injection and monitor mode.
- A WEP-encrypted wireless network to attack.

Step 1: Enable Monitor Mode and Capture Traffic

- Open a terminal and enter the following command to put the wireless adapter into monitor mode:

Command - airmon-ng start [interface]

- Replace [interface] with the name of your wireless adapter interface (such as wlan0).
- Use the following command to scan for wireless networks in monitor mode:

Command - airodump-ng [interface]

- This will display a list of wireless networks and their details, including the channel and BSSID (MAC address).
- Start capturing traffic from the target network using the following command:

Command - airodump-ng -c [channel] --bssid [BSSID] -w [filename] [interface]

- eplace [channel] with the channel of the target network, [BSSID] with the MAC address of the access point, [filename] with a name for the captured packets file, and [interface] with the name of your wireless adapter interface.

Step 2: Generate Traffic

- Use another device to generate traffic on the target network, such as streaming a video or downloading a file.
- This will generate more packets on the network and increase the chances of capturing enough packets for the attack.

Step 3: Analyze Captured Traffic

- After capturing enough traffic (at least several thousand packets), stop the capture process by pressing CTRL + C.
- Use the following command to view the captured packets:

Command - aircrack-ng -w [wordlist] [filename-01.cap]

- Replace [wordlist] with the path to a wordlist file, and [filename-01.cap] with the name of the captured packets file.
- This command will attempt to crack the WEP key using the captured packets and the specified wordlist.

Step 4: Perform the PTW or FMS Attack

- If the key was not cracked using the previous step, you can use a tool like Airdecap-ng to recover the WEP key using the PTW or FMS attack.
- Use the following command to recover the WEP key using the PTW attack:

Command - airdecap-ng -p [PTW] -e [ESSID] -n [ARP packets] -C [key stream file] -b [BSSID] [filename-01.cap]

- Replace [PTW] with the path to the PTW tool (included with Aircrack-ng), [ESSID] with the name of the target network, [ARP packets] with the number of ARP packets captured, [key stream file] with the name of the file containing the RC4 key stream, [BSSID] with the MAC address of the access point, and [filename-01.cap] with the name of the captured packets file.
- Use the following command to recover the WEP key using the FMS attack:

Command - airdecap-ng -p [FMS] -e [ESSID] -n [ARP packets] -C [key stream file] -b [BSSID] [filename-01.cap]

- Replace [FMS] with the path to the FMS tool (also included with Aircrack-ng), [ESSID] with the name of the target network, [ARP packets] with the number of ARP packets captured, [key stream file] with the name of the file containing the RC4 key stream, [BSSID] with the MAC address of the access point, and [filename-01.cap] with the name of the captured packets file.
- If the attack is successful, the WEP key will be displayed in the terminal output.

It's important to note that the effectiveness of these attacks can vary depending on factors such as the strength of the WEP key, the number of packets captured, and the quality of the wireless adapter used.

VII. Improved Attack on WEP

Unfortunately, after the release of the PTW attack, only little attention was drawn towards the old KoreK attack. Compared to the PTW attack, the KoreK attack has the advantage that it only needs the first two bytes of the keystreams of all captured packets. Usually, the recovery of the first two bytes of keystream is much easier than recovering the first 15 or 31 bytes. A pleasant exception is the work done by Vaudenay and Vuagnoux[16], who showed that the correlation used in the FMS attack can also be rewritten to vote for σi instead of Rk[i]. This correlation is one of the 17 correlations used in the KoreK attack.

To improve the performance of the PTW attack, we started rewriting all correlations used by KoreK to vote for σi instead of Rk[i]. Surprisingly, we where able to successfully modify almost all correlations used by KoreK, with a few exceptions: The correlations A 4 s13, A 4 u5 1, and A 4 u5 2 in the original KoreK attack can only be used to vote for Rk[1] when Rk[0] is known. Using these correlations for Rk[2], Rk[3] or any other keybyte besides Rk[1] has not been implemented by KoreK. The modification of these correlations results in new

correlations which vote only for σ1, even with Rk[0] or σ0 being unknown. KoreK assigned labels with comments to some correlations. The correlation A u5 3 is the only correlation labeled with the comment no good. When we tried to modify A u5 3 to vote for σi , the resulting correlation did not produce any useful results. The correlation A neg was used by KoreK to exclude values from being Rk[i]. The modification of this correlation results in a new correlation which can exclude values from being σi with a high probability. To implement this additional feature, a negative weight is assigned to this correlation. Another interesting extension of the PTW attack was suggested by [16] and [10] independently. First they showed that it is possible to get four times more votes for σ13 than for all other values of σi . This makes it much easier for an attacker to decide on the value of σ12 than all other values of σi . Secondly, they found out, that the correlation used in the PTW attack can easily be modified to vote for the value of σ12 + σi , even when the value of σ12 is unknown at this moment. After the attacker has decided on the value of σ12, he can get additional votes for each σi , by subtracting the value of σ12 from these votes. To use these additional correlations, an attacker needs the keystream bytes X[15] to X[30], which can sometimes be recovered too. Using all these ideas, we modified an implementation of the PTW attack1 resulting
in a new WEP cracking tool, which clearly needs fewer packets than previous implementations of the PTW attack. We decided to use the same key ranking strategy as used for the original PTW attack. We limited the number of keys the implementation tests before failing to 220. The same limit has been used by previous publications about WEP attacks, so that it should be easier to compare our attack to previous attacks. Figure 1 shows the success rate of our implementation. For a 50% success rate, the attack only needs about 24,200 packets, compared to 32,700 for the VX attack[16] and 35,000 to 40,000 for various implementations of the PTW attack [15, 14].

VIII. Conclusion

Wireless networks are seeing a growing amount of applications in the business world, as well as in the public and private sectors. Security is an important feature in wireless networks, as it ensures the transmission of data in a safe manner. The paper discusses the various classifications of attacks as well as the mechanisms that can be used to prevent them. Additionally, the paper discusses the vulnerabilities that are present in wireless devices.

Even though WEP's lack of security has been publicly known since 2001, we believe that key recovery attacks against WEP are still of interest. On the one hand, WEP is still used in the wild, and on the other, some companies are selling hardware using modified versions of the WEP protocol; these companies claim that their products are secure. Second, because the protocol used by WPA is not that dissimilar to that of WEP, it is possible for attacks on WEP to compromise the security of networks, as was demonstrated in the paper. Our attack demonstrates that not even WPA equipped with a robust password is completely secure and is vulnerable to attack in a situation that is representative of the real world. We recommend that vendors implement countermeasures against this attack, even though it is not a full-scale key recovery attack. We believe that updates can be easily developed and deployed with new drivers because the problem can be fixed in a high-level part of the protocol.

IX. REFERENCES

[1] Mohan V.Pawar, Anuradha J," Network Security and Types of Attacks in Network", International Conference on Computer, Communication and Convergence (ICCC 2015), volume 48, April 2015.

[2] Kuan Zhang,Student Member, IEEE, Xiaohui Liang,Member, IEEE,Rongxing Lu,Member, IEEE, and Xuemin Shen,Fellow IEEE," Sybil Attacks and Their Defenses in the Internet of Things", IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 5, OCTOBER 2014

[3] Yan Sun, Lihua Yin, Wenmao Liu," Defending sybil attacks in mobile social networks", Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on, 08 July 2014

[4] Deepti Sharma and Dr. Sanjay Thakur, "SybilDecline: A Survey on Novel Trusted Identity and Threshold Based Path Rank for Sybil Attack Identification in Social Network",International Journal of advanced research in Computer Science and engineering, Vol. 4, Issue 6, No., June 2014.

[5] Wei Chang, Jie Wu, Chiu C. Tan, and Feng Li," Sybil Defenses in Mobile Social Networks", IEEE GLOBECOM, December, 2013

[6] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail," A Study on the Vulnerability of AODV Routing Protocol to Resource Consumption Attack", Indian Journal of Science and Technology, Vol:5, Issue:11, November 2012.

[7] Kashif Laeeq,"Security Challenges & Preventions in Wireless Communications", International Journal of Scientific & Engineering Research Volume 2, Issue 5, May2011.

[8] Mehmud Abliz,"Internet denial of Service attacks and Defense Mechanism", Department of Computer Science, University of Pittsburgh,March 2011.

[9] K. kao, I-En Liao, Y-C Li, " Detecting rogue access points using client-side bottleneck bandwidth analysis,"ScienceDirect, computers & security 28 (2009).

[10] Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, Angelos D.Keromytis,"On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records".

[11] Rajani Muraleedharan, Yanjun Yan and Lisa Ann Osadciw," Detecting Sybil Attacks in Image Sensor Network Using Cognitive Intelligence", Department of Electrical Engineering and Computer Science Syracuse University, September 10, 2007.

[12] Esmiralda Moradian, Anne Håkansson," Possible attacks on XML Web Services", International Journal of Computer Science and Network Security, VOL.6 No.1B,January 2006.

[13] Heather D. Lane," Security Vulnerabilities and Wireless LAN Technology",

[14] Yuko Ozasa, Yoshiaki Fujikawa, Toshihiro Ohigashi, Hidenori Kuwakado, and Masakatu Morii. A study on the Tews, Weinmann, Pyshkin attack against WEP. In IEICE Tech. Rep., volume 107 of ISEC2007-47, pages 17–21, Hokkaido, July 2007. Thu, Jul 19, 2007 - Fri, Jul 20 : Future University-Hakodate (ISEC, SITE, IPSJ-CSEC).

[15] D. C. Plummer. RFC 826: Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware, November 1982.

[16] David Sterndark. Rc4 algorithm revealed. Usenet posting, Message-ID: , Sep 1994.

[17] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Transactions on Information and System Security, 7(2):319–332, May 2004.

[18] Erik Tews. Attacks on the wep protocol. Cryptology ePrint Archive, Report 2007/471, 2007. http://eprint.iacr.org/.

[19] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, WISA, volume 4867 of Lecture Notes in Computer Science, pages 188–202. Springer, 2007.

[20] Serge Vaudenay and Martin Vuagnoux. Passive-only key recovery attacks on RC4. In Selected Areas in Cryptography 2007, Lecture Notes in Computer Science. Springer, 2007.

[21] "Breaking 104-bit WEP in less than 60 seconds" by Andreas Klein https://www.cs.tau.ac.il/~tromer/papers/wep.pdf

[22] "Aircrack-ng" by Thomas d'Otreppe and Christophe Devine https://www.aircrack-ng.org/doku.php?id=aircrack-ng

[23] "WPA/WPA2 attacks and countermeasures" by Andrea Bittau, Mark Handley, and Joshua Lackey https://www.usenix.org/legacy/event/sec08/tech/full_papers/bittau/bittau.pdf

[24] "Practical attacks against WEP and WPA" by Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin https://eprint.iacr.org/2007/120.pdf

[25] "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2" by Mathy Vanhoef and Frank Piessens https://papers.mathyvanhoef.com/ccs2017.pdf